UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/893,501	06/29/2001	Todd Flemming	26509U	6332

20529 7590 01/11/2007

NATH & ASSOCIATES
112 South West Street
Alexandria, VA 22314

EXAMINER	
SHIFERAW, ELENI A	
ART UNIT	**PAPER NUMBER**
2136	

MAIL DATE	DELIVERY MODE
01/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

Advisory Action Before the Filing of an Appeal Brief	Application No.	Applicant(s)	
	09/893,501	FLEMMING, TODD	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 27 December 2006 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☒ The period for reply expires 3 months from the mailing date of the final rejection.
   b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered ~~and an explanation of how the new or amended claims would be rejected is provided below or appended~~.

   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *1-3,5,7-9,12-17 and 19-29*.
   Claim(s) withdrawn from consideration: *4, 6, 10, 11, and 18*.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

Continuation of 11. does NOT place the application in condition for allowance because: Regarding argument Mimura et al. failure to teach "...the integrator providing integration of the physical protection and information from the information asset protection module for making access decisions in accordance with usage patterns of the user to grant rights to the information systems..." as recited in claims 1, 12, and 20. Argument is not persuasive. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Mimura et al. discloses a security system wherein, when a staff enters a building, a smart card carried by the staff is verified and staff information inclusive of a staff number and fingerprint information is read from the smart card and is stored temporarily in a temporary storage file. When the staff logs on to a terminal, the fingerprint of the staff is read by a fingerprint input device and verified with the fingerprint information of the temporary storage file for verification (abstract). Leppek discloses monitoring user network resource usage activities and granting and/or denying access to another resources based on the user usage activities/patterns (see par. 0018-0020, and abstract). Sufficient motivation to combine is provided in the last office action page 5.

Regarding argument references failure to teach "transmitting a breach of physical asset protection in the centrally-located hosted environment ..." as recited in claims 1 and 12, argument is not persuasive. Mimura et al. discloses receiving the fingerprint, the access management device 185 verifies this fingerprint with the fingerprint recorded in the temporary file 145 in step 525. The access management device 185 outputs the code of the corresponding staff number when the coincident fingerprint exists in the temporary file 145, and outputs the code representing the verification failure when the coincident fingerprint does not exist. It records the verification result in the log file 180. The access management device 185 transmits the verification failure to the terminal 165 when the outputted code as the fingerprint verification result is the verification failure, and the verification success when the outputted code is the staff number, in step 535 and the terminal 165 generating deny access and an alarm. (see col. 7 lines 11-23).

Regarding argument Mimura et al. failure to disclose a processor based physical asset protection by triggering a user status change upon valid entry/exit through a door of a building, and no information asset protection reflected by the user status change updated to reflect changes in security access requirements, as recited in independent claims 1, 12, and 20, argument is not persuasive. Mimura et al. discloses a security system at the building door in advance and based on the authentication at the door and if the user is authentic/valid a staff information (staff number and fingerprint discrimination information) is stores temporarily in the temporary storage file 145 of the access management device 185 for later use when the user comes to the computer terminal 165, that has secure data, and request an access to secure data of terminal 165 (col. 5 lines 23-37). The staff information provided based on valid user door entry temporarily stored is used to provide user access to system resource/secure data at the terminal 165 upon normal logon (see col. 5 lines 50-col. 6 lines 67 and col. 7 lines 1-35). Temporarily stored staff information is erased when the user exits the door and when unauthorized user enters the building door with out being authenticated at the door and tries to access the secure resource terminal 165, he is denied access because the unauthorized user does not have the temporary stored staff information stored based on authentication at the door (see, col. 7 lines 11-23). Leppek discloses monitoring user network resource usage activities and granting and/or denying access to another resources based on the user usage activities/patterns (see par. 0018-0020, and abstract). Sufficient motivation to combine is provided in the last office action page 5.

Regarding argument Mimura et al. failure to teach access decisions in accordance with usage patterns of the user by using the integration of the processor to grant rights to the information systems, as recited in claims 1, 12, and 20, argument is not persuasive. Mimura et al. discloses access decisions based on user fingerprint/staff information input at the door and at the terminal based on temporarily stored staff information and/or when the staff logs on to a terminal, the fingerprint of the staff is read by a fingerprint input device and verified with the fingerprint information of the temporary storage file for verification (abstract). Leppek discloses monitoring user network resource usage activities and granting and/or denying access to another resources based on the user usage activities/patterns (see par. 0018-0020, and abstract). Sufficient motivation to combine is provided in the last office action page 5.

Regarding argument Leppek failure to teach usage patterns that applicant defines in the argument "repeat system", argument is not persuasive. Leppek discloses a network resource security services control system monitoring activity associated with a users attempt to and actual conducting of data communications (abstract). The event manager 240 is a routine that monitors network activity, in particular "events" occurring as a result of activity among users and resources of the network. An event is an activity that occurs when a user executes activity in the network, or a result of exercising or using a resource or object within the system (par. 0018). The event manager 240 takes action based on user users event "repeated" activity to give or deny access (par. 0018-0020).

Regarding applicant's argument Leppek failure to teach "...the present usage can be compared with historic usage and then re-calculating the usage pattern" as argued on remark page 5 last paragraph, argument is not persuasive because it is not claimed.

Regarding applicant's argument Leppek failure to teach "integration of physical and information security ... the transmit a breach of physical asset protection in the centrally-located hosted environment operates such that information asset protection is maintained by denying access" as recited in claims 1, 12, and 20, argument is not persuasive. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Mimura et al. teaches integration of physical and information security and/or a security system at the building door in advance and based on the authentication at the door and if the user is authentic/valid a staff information (staff number and fingerprint discrimination information) is stores temporarily in the temporary storage file 145 of the access management device 185 for later use when the user comes to the computer terminal 165, that has secure data, and request an access to secure data of terminal 165 (col. 5 lines 23-37). The staff information provided based on valid user door entry temporarily stored is used to provide user access to system resource/secure data at the terminal 165 upon normal logon (see col. 5 lines 50-col. 6 lines 67 and col. 7 lines 1-35). Temporarily stored staff information is erased when the user exits the door and when unauthorized user enters the building door with out being authenticated at the door and tries to access the secure resource terminal 165, he is denied access because the unauthorized user does not have the temporary stored staff information stored based on authentication at the door (see, col. 7 lines 11-23). And Leppek discloses monitoring user network resource usage activities and granting and/or denying access to another resources based on the user usage activities/patterns (see par. 0018-0020, and abstract). Sufficient motivation to combine is provided in the last office action page 5.

Accordingly, the rejections for claims 1-3, 5, 7-9, 12-17, and 19-29 are respectfully maintained..

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1/9/07